CVE SCANNER - NIST DATABASE

IT-Service Walter

Jörn Walter
www.it-service-walter.com
07.10.2025

DER CVE SCANNER – NIST DATABASE

ÜBERBLICK

DER **CVE VULNERABILITY SCANNER** IST EIN WINDOWS-TOOL ZUR ÜBERPRÜFUNG INSTALLIERTER SOFTWARE AUF BEKANNTE SICHERHEITSLÜCKEN (CVES - COMMON VULNERABILITIES AND EXPOSURES).

CVE Vulnerability Scanner - Benutzerhandbuch

Version 2.0
Autor: Jörn Walter - IT-Service-Walter.com
Stand: Oktober 2025

Inhaltsverzeichnis

Einführung

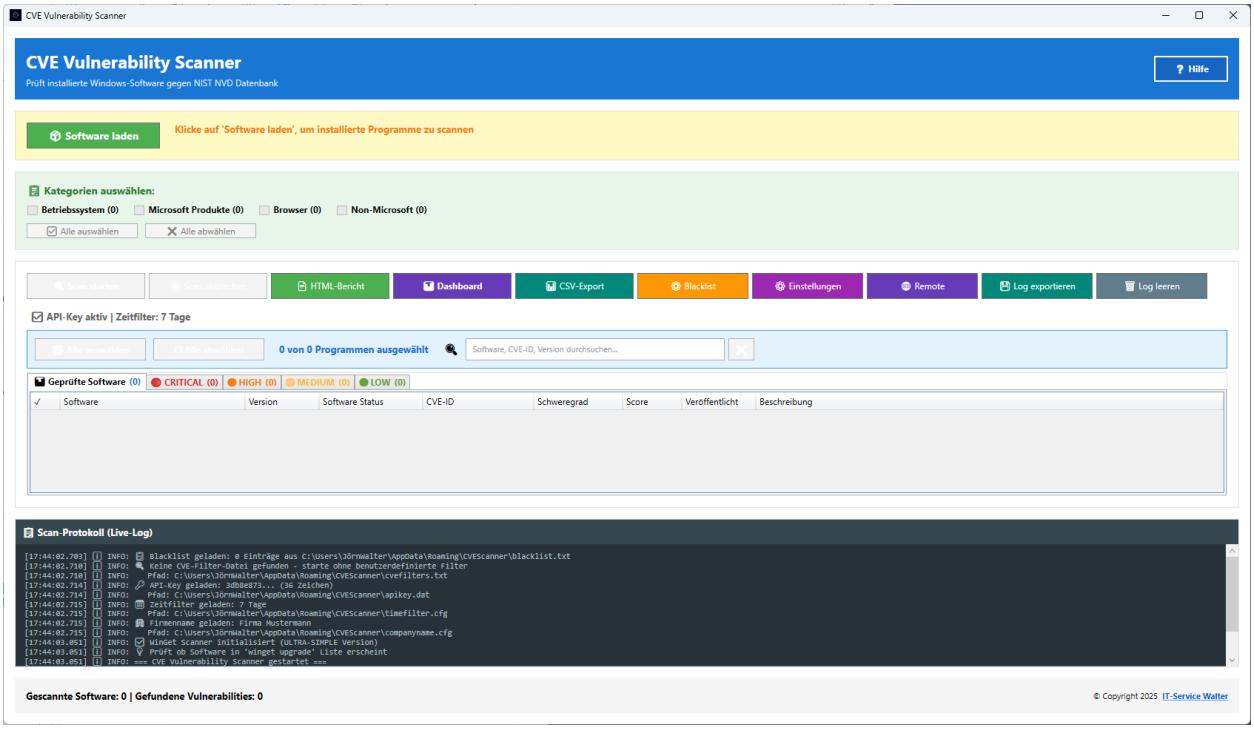
Der **CVE Vulnerability Scanner** ist ein Windows-Tool zur Überprüfung installierter Software auf bekannte Sicherheitslücken (CVEs - Common Vulnerabilities and Exposures).

Was macht das Tool?

- Erfasst alle auf Ihrem System installierten Programme
- Prüft diese gegen die NIST National Vulnerability Database (NVD)
- Identifiziert bekannte Sicherheitslücken
- Bewertet die Schwere der Schwachstellen (CRITICAL, HIGH, MEDIUM, LOW)
- Erstellt detaillierte Reports im HTML- und CSV-Format

Für wen ist das Tool gedacht?

- IT-Administratoren
- Security-Teams
- System-Verantwortliche
- Alle, die ihre Systemsicherheit überprüfen möchten



API-Key Verwaltung

Warum einen API-Key verwenden?

Die NVD API hat unterschiedliche Rate Limits:

Status	Requests pro 30 Sekunden	Empfehlung
Ohne API-Key	5	Nur für Tests
Mit API-Key	50	Produktiveinsatz

API-Key beantragen

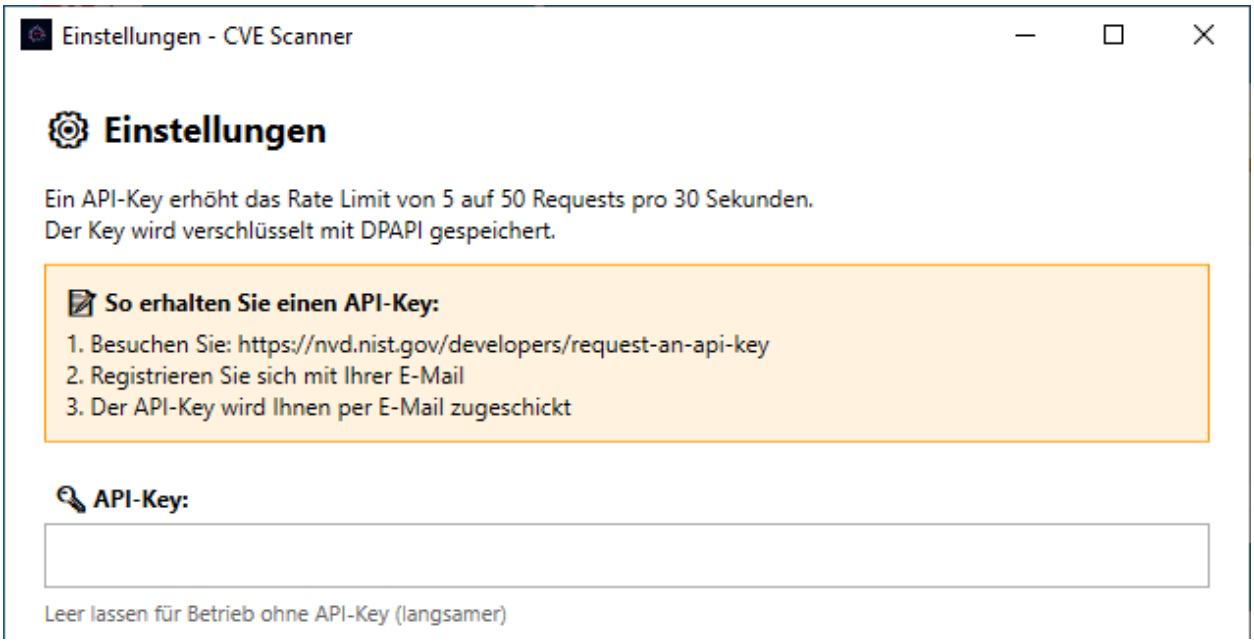
1. Besuchen Sie: https://nvd.nist.gov/developers/request-an-api-key
2. Füllen Sie das Formular aus (E-Mail-Adresse erforderlich)
3. Sie erhalten den Key innerhalb weniger Minuten per E-Mail
4. Der Key ist **kostenlos**

API-Key im Tool speichern

1. Kopieren Sie den erhaltenen API-Key
2. Fügen Sie ihn in das Feld "API-Key Verwaltung" ein
3. Klicken Sie auf **"Speichern"**
4. Status-Meldung: "✓ Gespeichert" (grün)
5. Der Delete-Button wird aktiviert

API-Key löschen

1. Klicken Sie auf **"Löschen"**
2. Bestätigen Sie die Sicherheitsabfrage
3. Das Feld wird geleert
4. Status: "Gelöscht"



Wo wird der API-Key gespeichert?

Speicherort:

%APPDATA%\CVEScanner\apikey.dat

Typischer Pfad:

C:\Users\[IhrBenutzername]\AppData\Roaming\CVEScanner\config.xml

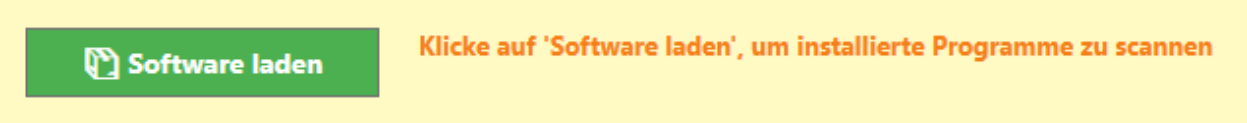
Sicherheit:

- Der Key wird **verschlüsselt** gespeichert (Windows DPAPI)
- Nur Ihr Benutzer auf diesem Computer kann ihn entschlüsseln
- Kein Klartext in der Datei

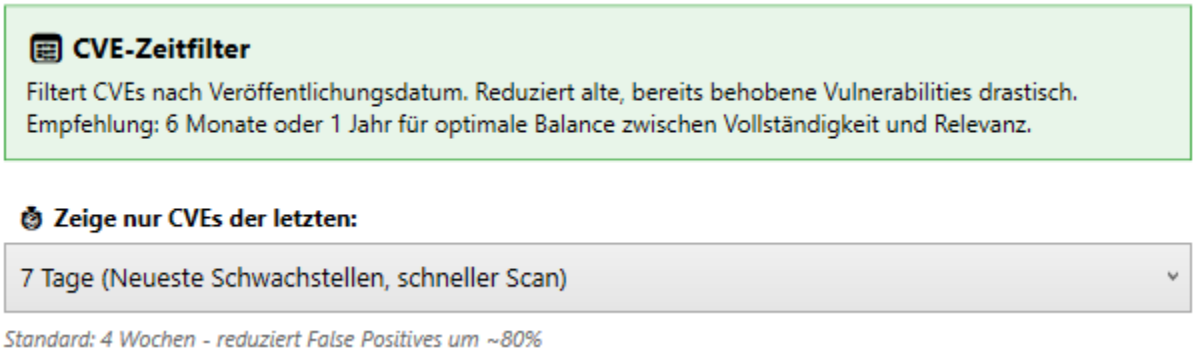
Software-Inventarisierung

Software laden

1. Klicken Sie auf **"Software laden"** (grüner Button)



2. Wählen Sie im Tab **"Einstellungen"** den Zeitraum (siehe nächster Abschnitt)
   Das System durchsucht:
   - Windows Registry (HKLM und HKCU)
   - Installierte Windows Apps (AppX)



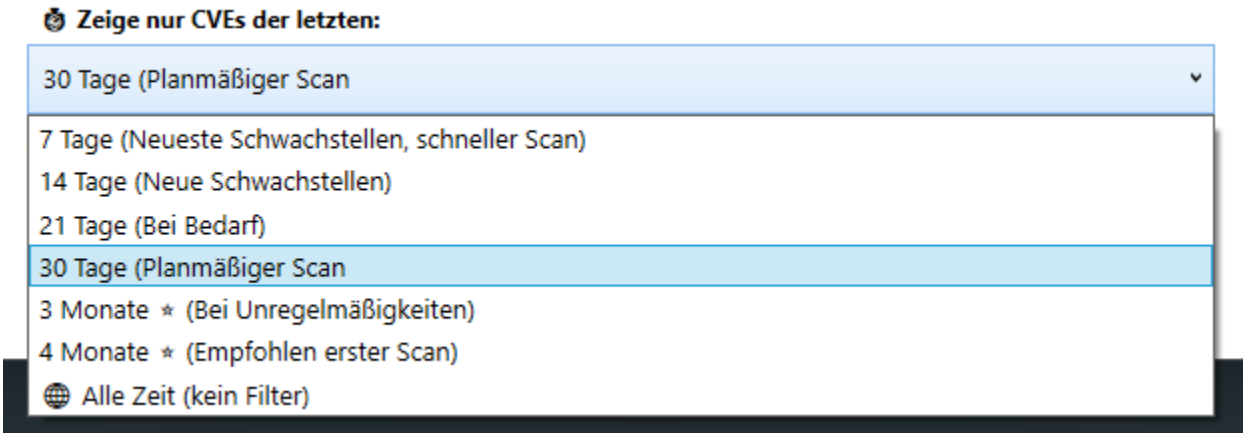
3. Fortschritt wird im Log-Tab angezeigt
4. Nach Abschluss: Anzahl der gefundenen Programme wird angezeigt

Was wird erfasst?

- Alle über die Systemsteuerung installierten Programme
- Windows Store Apps
- 64-bit und 32-bit Programme
- Programme im Benutzer- und Systemkontext

Zeitraum-Auswahl

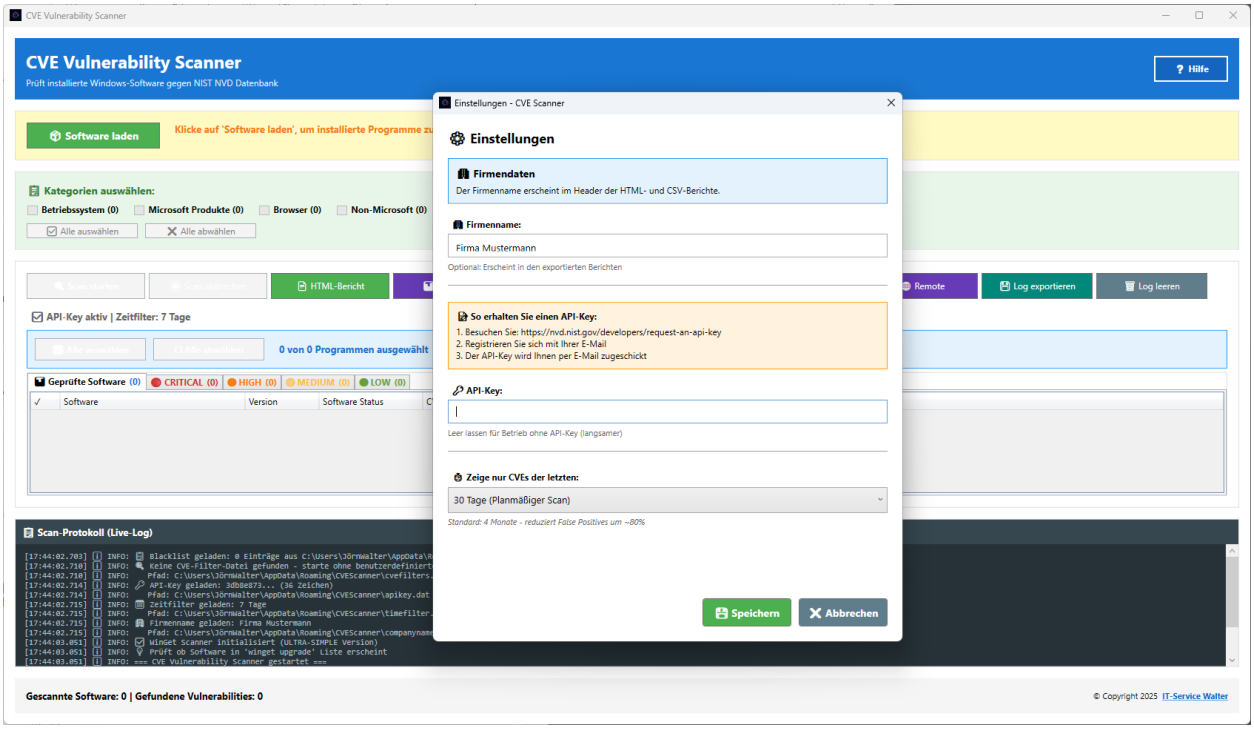
Vor dem Software-Laden können Sie den Scan-Zeitraum festlegen:



Zeitraum	Verwendungszweck
1 Woche	Neueste Schwachstellen, schneller Scan
2 Wochen	Neue Schwachstellen
3 Wochen	Neue Schwachstellen bei Bedarf
4 Wochen	Planmäßiger Scan (empfohlen)
3 Monate	Bei unregelmäßigem Scanverhalten
1 Jahr	Empfohlen erster Scan

Standard: 4 Wochen (empfohlen für ausgewogene Ergebnisse)

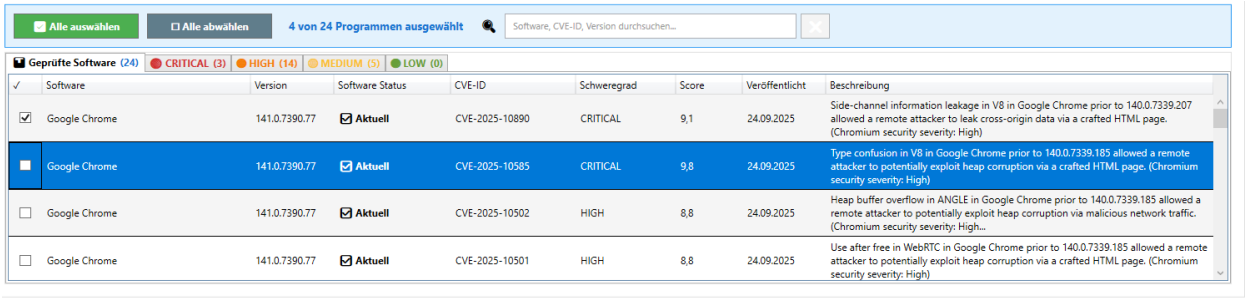
1. Für eine detaillierte Analyse lassen, die die empfohlene Abfragemethode aktiviert.



Software-Auswahl und Filter

Manuelle Auswahl

- Aktivieren Sie die Checkbox vor jedem Programm
- Mehrfachauswahl per Strg+Klick möglich
- Auswahl-Zähler oben rechts: "Ausgewählt: X"



Schnellfilter-Buttons

"✓ Alle"

- Wählt alle sichtbaren Programme aus
- Berücksichtigt aktive Textfilter

"✗ Keine"

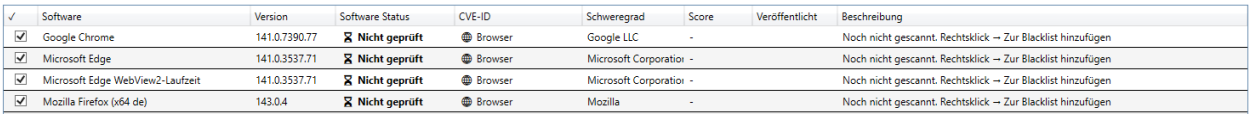
- Deaktiviert alle Auswahlhäkchen

"Microsoft"

- Wählt alle Microsoft-Produkte aus
- Sucht nach "Microsoft" und "Windows" im Namen

"Browser"

- Wählt alle Browser aus
- Erfasst: Chrome, Firefox, Edge, Opera, Brave



"Non-Microsoft"

- Wählt alle Nicht-Microsoft-Programme aus

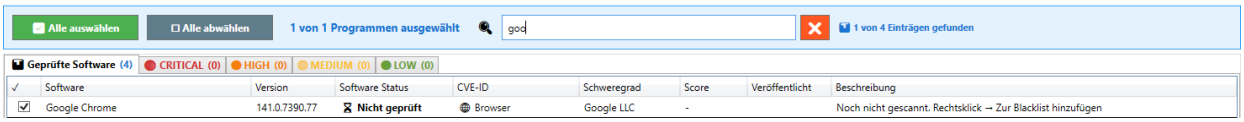
- Prüft sowohl Programmname als auch Hersteller

Textsuche-Filter

Suchfeld oben links:

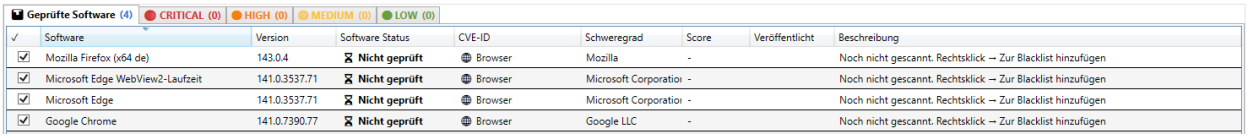
- Filtert die Liste in Echtzeit
- Durchsucht Programmname und Hersteller
- Groß-/Kleinschreibung wird ignoriert
- Beispiel: "UPD" zeigt alle UPDF-Programme

Tipp: Kombinieren Sie Textsuche mit Schnellfiltern für präzise Auswahl



Spalten sortieren

- Klicken Sie auf die Spaltenüberschriften zum Sortieren
- Verfügbare Spalten:
    - **Software:** Programmname
    - **Version:** Versionsnummer
    - **Hersteller:** Publisher/Hersteller



CVE-Scan durchführen

Voraussetzungen

- Mindestens ein Programm muss ausgewählt sein
- Internetverbindung muss aktiv sein
- Button **"Scan starten"** ist aktiviert (blau)

Scan starten

1. Klicken Sie auf **"▶️ Scan starten"**
2. Das Tool wechselt automatisch zum Tab **"Scan-Ergebnisse"**
3. Der Fortschritt wird angezeigt

Was passiert während des Scans?

Für jedes ausgewählte Programm:

1. Anfrage an die NVD API
2. Suche nach CVEs im gewählten Zeitraum
3. Analyse der Schweregrade
4. Speicherung der Ergebnisse

Fortschrittsanzeige:

- Aktuell geprüftes Programm wird angezeigt
- Format: "Prüfe: [Programmname] (X/Y)"

Scan-Dauer

Ohne API-Key:

- Ca. 6 Sekunden pro Programm (5 Requests/30s)
- 100 Programme ≈ 10 Minuten

Mit API-Key:

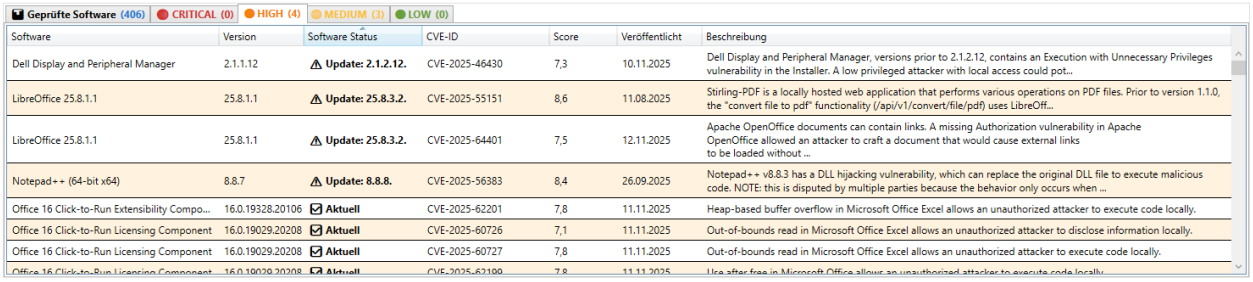
- Ca. 0,6 Sekunden pro Programm (50 Requests/30s)
- 100 Programme ≈ 1 Minute

Scan-Ergebnisse interpretieren

Statistik-Übersicht

Oben im Ergebnisse-Tab sehen Sie fünf Kennzahlen:

Kennzahl	Bedeutung
Geprüfte Software	Anzahl gescannter Programme
CRITICAL	Kritische Schwachstellen (Score 9.0-10.0)
HIGH	Hohe Schwachstellen (Score 7.0-8.9)
MEDIUM	Mittlere Schwachstellen (Score 4.0-6.9)
LOW	Niedrige Schwachstellen (Score 0.1-3.9)



Severity-Level verstehen

CRITICAL (Rot)

- Höchste Priorität
- Sofortige Handlung erforderlich
- Oft remote ausnutzbar ohne Authentifizierung
- **Beispiele:** Remote Code Execution, SQL Injection

HIGH (Orange)

- Hohe Priorität
- Zeitnahe Behebung empfohlen
- Meist remote ausnutzbar oder mit geringen Hürden
- **Beispiele:** Privilege Escalation, XSS

MEDIUM (Gelb)

- Mittlere Priorität
- Behebung im nächsten Patch-Zyklus
- Oft lokal ausnutzbar oder spezielle Bedingungen nötig
- **Beispiele:** Information Disclosure, DoS

LOW (Grün)

- Niedrige Priorität
- Zur Kenntnis nehmen, nicht dringend
- Meist theoretische Risiken
- **Beispiele:** Minor Information Leaks

Ergebnistabelle

Spalten:

- **Software:** Name des betroffenen Programms
- **Version:** Installierte Version
- **Software-Status:** Gibt aus, ob die Software aktuell ist
- **CVE-ID:** Eindeutige CVE-Nummer
- **Severity:** Schweregrad (farbcodiert)
- **Score:** CVSS-Score (0.0-10.0)
- **Beschreibung:** Details zur Schwachstelle

Sortierung:

- Standard: Nach Score absteigend (kritischste zuerst)
- Klick auf Spaltenüberschrift für andere Sortierung

CVE-IDs nachschlagen

Klicken Sie auf eine CVE-ID in dem HTML-Bericht, um:

- Details auf nvd.nist.gov zu öffnen
- Vollständige Beschreibung zu lesen
- Patches und Mitigations zu finden
- Betroffene Versionen zu prüfen

Software	Version	Software Status	CVE-ID	Schweregrad	Score	Veröffentlicht	Beschreibung
Google Chrome	141.0.7390.77	☑ Aktuell	CVE-2025-10890	CRITICAL	9,1	24.09.2025	Side-channel information leakage in V8 in Google Chrome prior to 140.0.7339.207 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)
Google Chrome	141.0.7390.77	☑ Aktuell	CVE-2025-10585	CRITICAL	9,8	24.09.2025	Type confusion in V8 in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
Google Chrome	141.0.7390.77	☑ Aktuell	CVE-2025-10502	HIGH	8,8	24.09.2025	Heap buffer overflow in ANGLE in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: High...

Ergebnisse exportieren

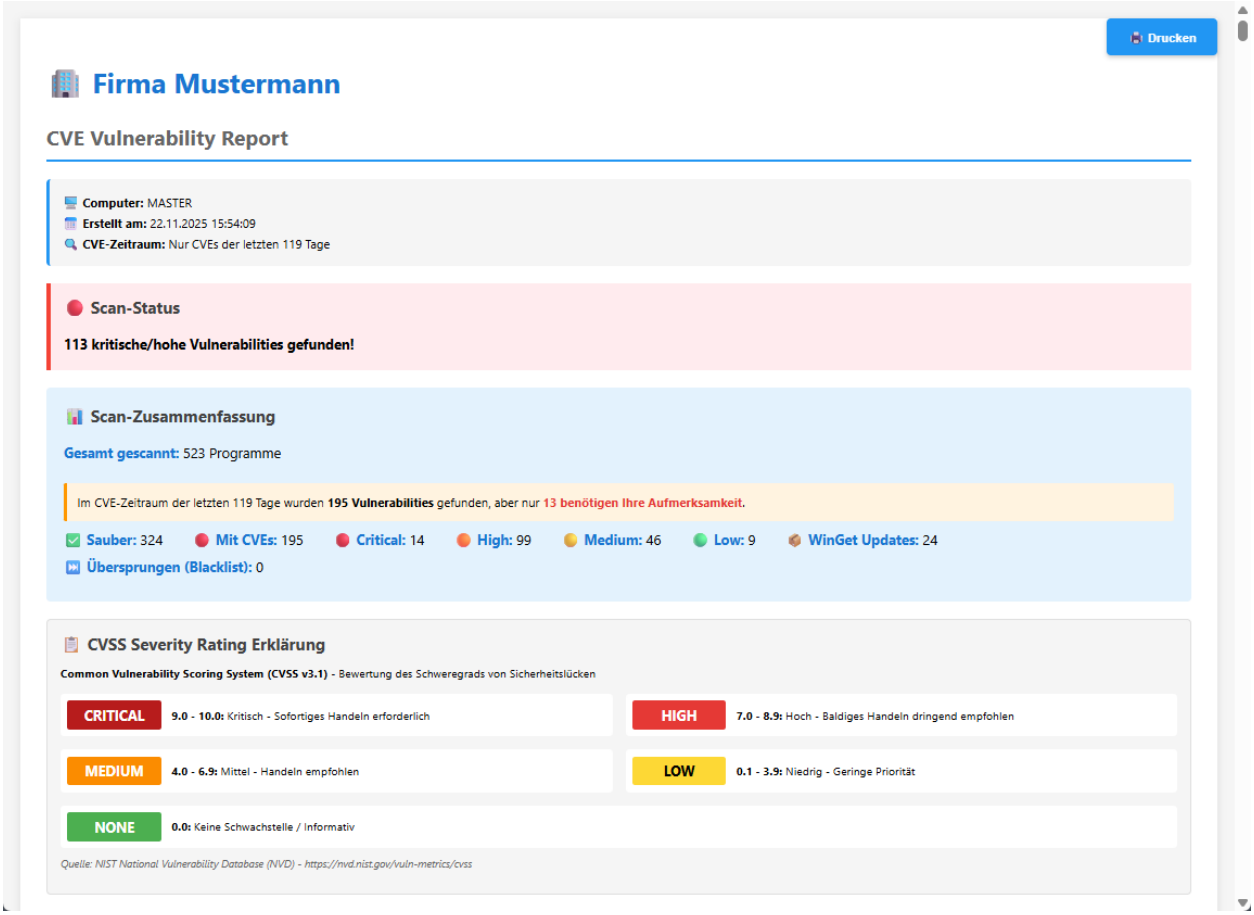
HTML-Report erstellen

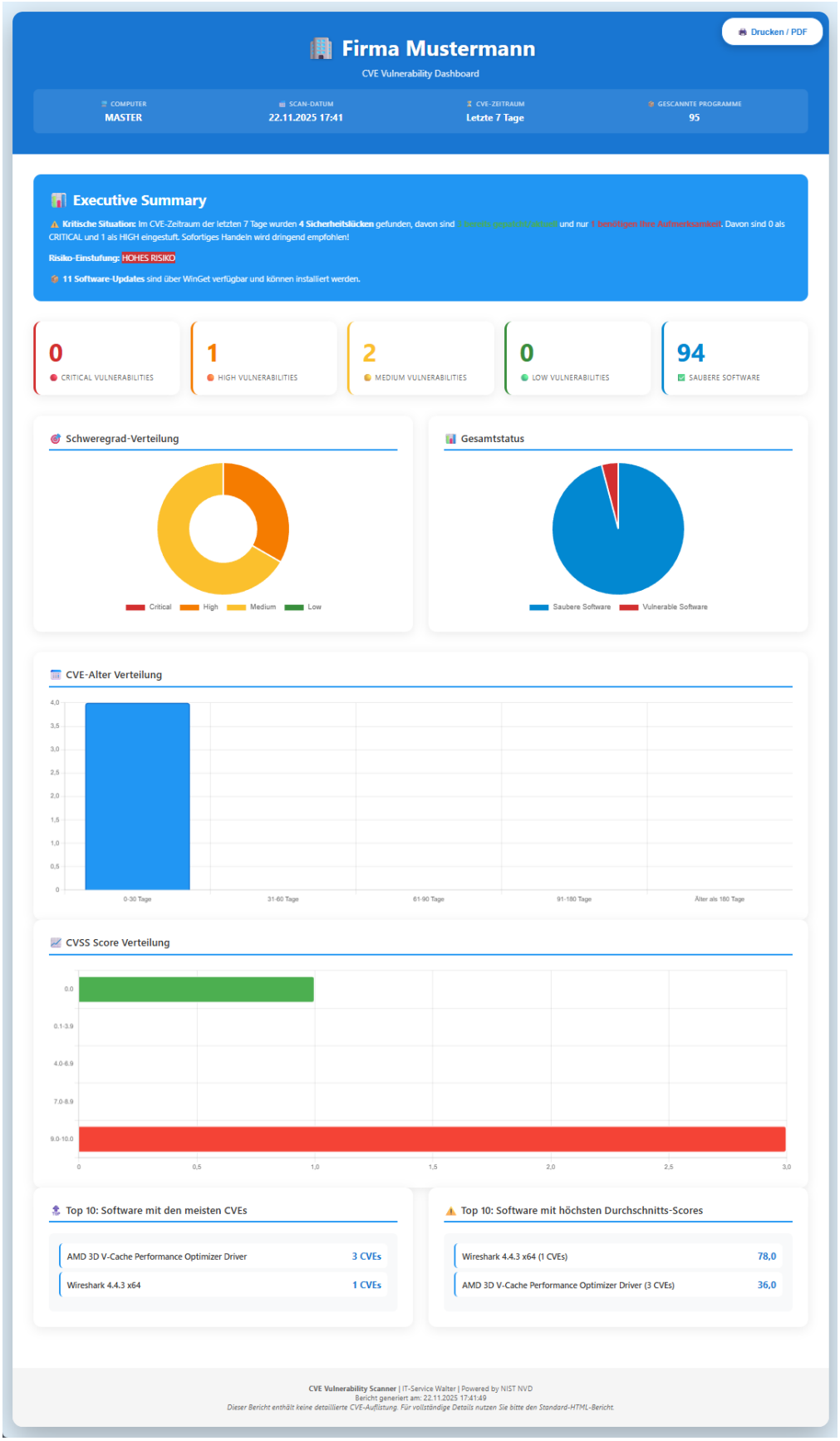
Automatisch:

- Wird nach jedem erfolgreichen Scan zum Speichern vorbereitet
- Speicherort: Desktop
- Dateiname: CVE-Report_Zeitstempel.html

Inhalt des Reports:

- Zusammenfassung (Datum, Zeitraum, Anzahl)
- Statistik-Dashboard mit farbigen Boxen
- Vollständige Ergebnistabelle
- Alle CVE-Details inkl. Beschreibungen
- Druckfunktion integriert




Drucken / PDF
Firma Mustermann
CVE Vulnerability Dashboard
COMPUTER
MASTER
SCAN-DATUM
22.11.2025 17:41
CVE-ZEITRAUM
Letzte 7 Tage
GESCANNTE PROGRAMME
95
Executive Summary
Kritische Situation: Im CVE-Zeitraum der letzten 7 Tage wurden 4 Sicherheitslücken gefunden, davon sind 3 bereits gepatcht/aktualisiert und nur 1 benötigen Ihre Aufmerksamkeit. Davon sind 0 als CRITICAL und 1 als HIGH eingestuft. Sofortiges Handeln wird dringend empfohlen!
Risiko-Einstufung: HOHES RISIKO
11 Software-Updates sind über WinGet verfügbar und können installiert werden.
0
CRITICAL VULNERABILITIES
1
HIGH VULNERABILITIES
2
MEDIUM VULNERABILITIES
0
LOW VULNERABILITIES
94
SAUBERE SOFTWARE
Schweregrad-Verteilung
Critical
High
Medium
Low
Gesamtstatus
Saubere Software
Vulnerable Software
CVE-Alter Verteilung
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
0-30 Tage
31-60 Tage
61-90 Tage
91-180 Tage
Älter als 180 Tage
CVSS Score Verteilung
0.0
0.1-3.9
4.0-6.9
7.0-8.9
9.0-10.0
0
0,5
1,0
1,5
2,0
2,5
3,0
Top 10: Software mit den meisten CVEs
AMD 3D V-Cache Performance Optimizer Driver
3 CVEs
Wireshark 4.4.3 x64
1 CVEs
Top 10: Software mit höchsten Durchschnitts-Scores
Wireshark 4.4.3 x64 (1 CVEs)
78,0
AMD 3D V-Cache Performance Optimizer Driver (3 CVEs)
36,0
CVE Vulnerability Scanner | IT-Service Walter | Powered by NIST NVD
Bericht generiert am: 22.11.2025 17:41:49
Dieser Bericht enthält keine detaillierte CVE-Auflistung. Für vollständige Details nutzen Sie bitte den Standard-HTML-Bericht.

CSV-Export

Verwendung:

- Für Excel-Auswertungen
- Für Ticketsysteme
- Für Datenbank-Imports

Export durchführen:

1. Klicken Sie auf **" 📊 CSV"**
2. Speicherdialog öffnet sich
3. Wählen Sie Speicherort und Dateiname
4. Standard: CVE-Scan-YYYY-MM-DD.csv

CSV-Format:

- Trennzeichen: Semikolon (;)
- Encoding: UTF-8
- Spalten: Software, Version, Software-Status,CVE_ID, Severity, Score, Beschreibung

In Excel öffnen:

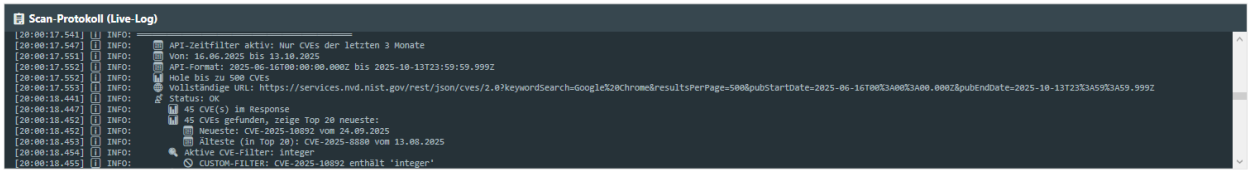
1. Excel starten
2. Datei → Öffnen → CSV-Datei auswählen
3. Textimport-Assistent: Trennzeichen "Semikolon" wählen,

Software	Version	Software Status	CVE-ID	Schweregrad	CVSS Score	Veröffentlicht	Beschreibung	NVD Link
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-10585	CRITICAL	9,8	24.09.2025	Type confusion in V8 in Google Chrome prior	https://nvd.nist.gov/vuln/detail/CVE-2025-10585
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-4609	CRITICAL	9,6	22.08.2025	Incorrect handle provided in unspecified circ	https://nvd.nist.gov/vuln/detail/CVE-2025-4609
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-10890	CRITICAL	9,1	24.09.2025	Side-channel information leakage in V8 in G	https://nvd.nist.gov/vuln/detail/CVE-2025-10890
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-10502	HIGH	8,8	24.09.2025	Heap buffer overflow in ANGLE in Google Chr	https://nvd.nist.gov/vuln/detail/CVE-2025-10502
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-10501	HIGH	8,8	24.09.2025	Use after free in WebRTC in Google Chrome p	https://nvd.nist.gov/vuln/detail/CVE-2025-10501
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-10500	HIGH	8,8	24.09.2025	Use after free in Dawn in Google Chrome prio	https://nvd.nist.gov/vuln/detail/CVE-2025-10500
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-10200	HIGH	8,8	10.09.2025	Use after free in Serviceworker in Google Chr	https://nvd.nist.gov/vuln/detail/CVE-2025-10200
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-9866	HIGH	8,8	03.09.2025	Inappropriate implementation in Extensions	https://nvd.nist.gov/vuln/detail/CVE-2025-9866
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-9864	HIGH	8,8	03.09.2025	Use after free in V8 in Google Chrome prior to	https://nvd.nist.gov/vuln/detail/CVE-2025-9864
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-9478	HIGH	8,8	26.08.2025	Use after free in ANGLE in Google Chrome pri	https://nvd.nist.gov/vuln/detail/CVE-2025-9478
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-9132	HIGH	8,8	20.08.2025	Out of bounds write in V8 in Google Chrome p	https://nvd.nist.gov/vuln/detail/CVE-2025-9132
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-8901	HIGH	8,8	13.08.2025	Out of bounds write in ANGLE in Google Chro	https://nvd.nist.gov/vuln/detail/CVE-2025-8901
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-8882	HIGH	8,8	13.08.2025	Use after free in Aura in Google Chrome prior	https://nvd.nist.gov/vuln/detail/CVE-2025-8882
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-8880	HIGH	8,8	13.08.2025	Race in V8 in Google Chrome prior to 139.0.7	https://nvd.nist.gov/vuln/detail/CVE-2025-8880
Microsoft Edge	141.0.3537.71	Aktuell	CVE-2025-49713	HIGH	8,8	02.07.2025	Access of resource using incompatible type (	https://nvd.nist.gov/vuln/detail/CVE-2025-49713
Microsoft Edge	141.0.3537.71	Aktuell	CVE-2025-59251	HIGH	7,6	24.09.2025	Microsoft Edge (Chromium-based) Remote C	https://nvd.nist.gov/vuln/detail/CVE-2025-59251
Microsoft Edge	141.0.3537.71	Aktuell	CVE-2025-49741	HIGH	7,4	01.07.2025	No cwe for this issue in Microsoft Edge (Chro	https://nvd.nist.gov/vuln/detail/CVE-2025-49741
Google Chrome	141.0.7390.77	Aktuell	CVE-2025-8881	MEDIUM	6,5	13.08.2025	Inappropriate implementation in File Picker	https://nvd.nist.gov/vuln/detail/CVE-2025-8881
Microsoft Edge	141.0.3537.71	Aktuell	CVE-2025-47963	MEDIUM	6,3	11.07.2025	No cwe for this issue in Microsoft Edge (Chro	https://nvd.nist.gov/vuln/detail/CVE-2025-47963
Microsoft Edge	141.0.3537.71	Aktuell	CVE-2025-47182	MEDIUM	5,6	11.07.2025	Improper input validation in Microsoft Edge (	https://nvd.nist.gov/vuln/detail/CVE-2025-47182
Microsoft Edge	141.0.3537.71	Aktuell	CVE-2025-47964	MEDIUM	5,4	11.07.2025	Microsoft Edge (Chromium-based) Spoofing	https://nvd.nist.gov/vuln/detail/CVE-2025-47964
Microsoft Edge	141.0.3537.71	Aktuell	CVE-2025-53791	MEDIUM	4,7	05.09.2025	Improper access control in Microsoft Edge (C	https://nvd.nist.gov/vuln/detail/CVE-2025-53791
Microsoft Edge WebView2-Laufzeit	141.0.3537.71	Aktuell	SAUBER	Keine CVEs	0.0	-	Keine CVEs in den letzten 3 Monate gefunden	
Mozilla Firefox (x64 de)	143.0.4	Aktuell	CVE-2025-50185	UNKNOWN	0	26.07.2025	DbGate is cross-platform database manager	https://nvd.nist.gov/vuln/detail/CVE-2025-50185

Log-Funktion

Log-Tab öffnen

- Klicken Sie auf den Tab " 📝 **Log"**
- Zeigt alle Aktivitäten in chronologischer Reihenfolge



Was wird geloggt?

Software-Laden:

[19:59:57.893] ℹ️ INFO: 📋 Blacklist geladen: 1 Einträge aus C:\Users\JörnWalter\AppData\Roaming\CVEScanner\blacklist.txt

[19:59:57.901] ℹ️ INFO: 🔍 CVE-Filter geladen: 1 Einträge aus C:\Users\JörnWalter\AppData\Roaming\CVEScanner\cvefilters.txt

[19:59:57.904] ℹ️ INFO: 🔑 API-Key geladen: 3db8e873... (36 Zeichen)

[19:59:57.904] ℹ️ INFO: Pfad: C:\Users\JörnWalter\AppData\Roaming\CVEScanner\apikey.dat

[19:59:57.905] ℹ️ INFO: 🗓️ Zeitfilter geladen: 3 Monate

CVE-Scan:

[20:00:21.736] ℹ️ INFO: 🔍 Optimierte Suche: 'Mozilla Firefox (x64 de)' → 'Mozilla Firefox'

[20:00:21.737] ℹ️ INFO: 🗓️ API-Zeitfilter aktiv: Nur CVEs der letzten 3 Monate

[20:00:21.737] ℹ️ INFO: 🗓️ Von: 16.06.2025 bis 13.10.2025

[20:00:21.737] ℹ️ INFO: 🗓️ API-Format: 2025-06-16T00:00:00.000Z bis 2025-10-13T23:59:59.999Z

[20:00:21.738] ℹ️ INFO: 📊 Hole bis zu 500 CVEs

[20:00:21.738] ℹ️ INFO: 🌐 Vollständige URL: https://services.nvd.nist.gov/rest/json/cves/2.0?keywordSearch=Mozilla%20Firefox&resultsPerPage=500&pubStartDate=2025-06-16T00%3A00%3A00.000Z&pubEndDate=2025-10-13T23%3A59%3A59.999Z

[20:00:22.409] ℹ️ INFO: 📡 Status: OK

Log speichern

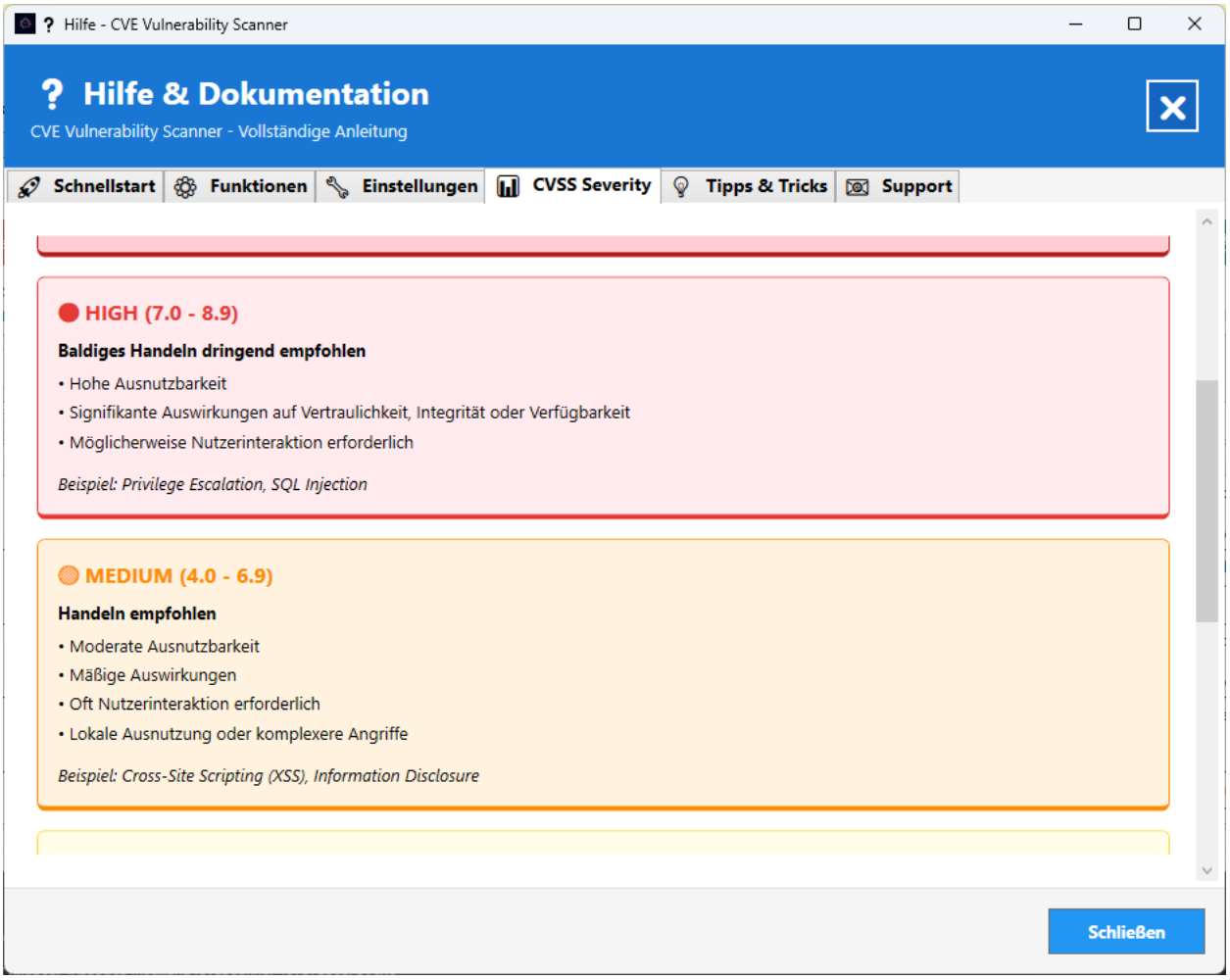
Manuell:

1. Markieren Sie den gewünschten Text
2. Strg+C zum Kopieren
3. In Texteditor einfügen und speichern
4. Oder Sie nutzen die Funktion Log exportieren

Hilfe-Funktion

Hilfe öffnen

- Klicken Sie auf "❓ **Hilfe**" (oben rechts im Header)
- Ein separates Fenster öffnet sich



Hilfe-Inhalte

API-Key Konfiguration:

- Rate Limits erklärt
- Beantragungslink
- Vorteile des API-Keys

Bedienungsanleitung:

- 7-Schritte-Anleitung
- Von Software-Laden bis Export

Weitere Informationen:

- Links zur NVD-Dokumentation
- Alle Links sind klickbar

Über dieses Tool:

- Kontaktdaten (IT-Service Walter)
- Website-Link
- E-Mail-Link

Datenspeicherung und Sicherheit

Gespeicherte Daten

API-Key & weitere Konfigurationen:

- Pfad: %APPDATA%\CVEScanner\
- Verschlüsselt mit Windows DPAPI
- Nur für Ihren Benutzer lesbar

HTML-Report:

- Pfad: %USERPROFILE%\Desktop\CVE_Report_20251013_195348.html
- Klartext (keine sensiblen Daten)

CSV-Export:

- Benutzer wählt Speicherort
- Vorbereitet für den Import im Microsoft Excel

Sicherheitshinweise

Der Scanner:

- Installiert keine Software
- Ändert keine Systemeinstellungen
- Sammelt keine personenbezogenen Daten
- Sendet nur Programmnamen an NVD API
- Prüft über WinGet die Softwareversion
- Keine Telemetrie oder Tracking

Ihre Daten:

- Bleiben auf Ihrem Computer
- API-Key wird verschlüsselt gespeichert

NVD API:

- NIST ist eine US-Regierungsbehörde
- API ist öffentlich und kostenlos
- Keine Authentifizierung ohne Key erforderlich
- Datenschutzrichtlinien: https://nvd.nist.gov/general/privacy-policy

Daten löschen

API-Key löschen:

- Über die Einstellungen
- Oder Datei manuell löschen: %APPDATA%\CVEScanner\apikey.dat

Reports löschen:

- Manuell vom Desktop löschen

Fehlerbehebung

"Timeout" bei einzelnen Programmen

Ursache: NVD API antwortet nicht rechtzeitig
Lösung:

- Normal bei Netzwerkproblemen
- Betroffenes Programm wird übersprungen
- Scan läuft weiter

API-Rate-Limit erreicht

Symptom: Sehr langsamer Scan trotz API-Key
Lösung:

1. Prüfen Sie, ob API-Key korrekt gespeichert ist
2. Status sollte "🔑 API-Key geladen" zeigen
3. Key evtl. neu eingeben und speichern

Software-Liste bleibt leer

Ursache: Berechtigungsproblem oder Registry-Fehler
Lösung:

1. Als Administrator ausführen
2. Antivirus temporär deaktivieren
3. Log-Tab auf Fehlermeldungen prüfen

Keine CVEs gefunden (unerwartetes Ergebnis)

Mögliche Gründe:

- Gewählter Zeitraum zu kurz (7 Tage)
- Software ist aktuell und hat keine neuen CVEs
- Programmnamen stimmen nicht mit NVD überein

Empfehlung:

- Zeitraum auf 90 oder 120 Tage erhöhen
- Bekannt anfällige Software testen (z.B. ältere Browser)

Systemvoraussetzungen

- Ab Windows 10 aufwärts
- Microsoft Windows Desktop Runtime 8.x (x64)

Häufig gestellte Fragen

Brauche ich zwingend einen API-Key?

Nein, aber es wird empfohlen:

- Ohne Key: 5 Requests/30s (sehr langsam)
- Mit Key: 50 Requests/30s (10x schneller)
- Key ist kostenlos

Wie lange dauert ein typischer Scan?

Mit API-Key:

- 10 Programme: ~10 Sekunden
- 50 Programme: ~30 Sekunden
- 100 Programme: ~1 Minute

Ohne API-Key:

- 10 Programme: ~1 Minute
- 50 Programme: ~5 Minuten
- 100 Programme: ~10 Minuten

Kann ich den Scan abbrechen?

- Scan abbrechen klicken

Werden Patches erkannt?

Nein. Das Tool prüft nur:

- Programmnamen
- Zeitraum für CVE-Veröffentlichung

Es prüft **nicht**:

- Ob ein Patch installiert ist
- Die genaue Versionsnummer gegen CVE-Ranges

Hinweis: Eine gefundene CVE bedeutet nicht zwingend, dass Ihr System verwundbar ist. Prüfen Sie die CVE-Details.

Was bedeutet "UNKNOWN" bei Severity?

Die CVE hat noch keine CVSS-Bewertung in der NVD. Das kann vorkommen bei:

- Sehr neuen CVEs
- CVEs im Analyse-Status
- Fehlenden Metriken

Kann ich mehrere Computer scannen?

Ja, kopieren Sie das Skript auf jeden Computer und führen Sie es dort aus. Jedes System muss einzeln gescannt werden.

Werden auch portable Apps erfasst?

Nein, nur Programme die:

- In der Registry registriert sind
- Als Windows App installiert sind

Portable/ZIP-Versionen werden nicht erkannt.

Funktioniert das Tool offline?

Nein, es benötigt:

- Internetverbindung zur NVD API
- Zugriff auf https://services.nvd.nist.gov

Gibt es Support?

Kontakt:

- Web: https://www.it-service-walter.com
- E-Mail: info@it-service-walter.com

Anhang: CVSS Score-System

Das Common Vulnerability Scoring System (CVSS) bewertet Schwachstellen von 0.0 bis 10.0:

Score	Rating	Farbe	Aktion
9.0-10.0	CRITICAL	Rot	Sofort patchen
7.0-8.9	HIGH	Orange	Zeitnah patchen
4.0-6.9	MEDIUM	Gelb	Nächster Patch-Zyklus
0.1-3.9	LOW	Blau	Zur Kenntnis
0.0	NONE	Grau	Kein Risiko

Faktoren für den Score:

- Angriffsvektor (Netzwerk/lokal)
- Komplexität des Angriffs
- Erforderliche Privilegien
- Auswirkung auf Vertraulichkeit
- Auswirkung auf Integrität
- Auswirkung auf Verfügbarkeit

Glossar

API: Application Programming Interface - Schnittstelle zum Datenaustausch

CVE: Common Vulnerabilities and Exposures - Eindeutige ID für Schwachstellen

CVSS: Common Vulnerability Scoring System - Bewertungssystem für Schwachstellen

NVD: National Vulnerability Database - US-Regierungsdatenbank für CVEs

NIST: National Institute of Standards and Technology - US-Standardisierungsbehörde

Rate Limit: Maximale Anzahl von API-Anfragen pro Zeiteinheit

Severity: Schweregrad einer Schwachstelle

DPAPI: Data Protection API - Windows-Verschlüsselungsfunktion

---

Ende des Handbuchs

Für weitere Unterstützung kontaktieren Sie bitte:
IT-Service Walter
Jörn Walter
Mittelstr. 65, 53879 Euskirchen
Web: https://www.it-service-walter.com
E-Mail: info@it-service-walter.com

Verkauf

Als Firmenlizenz einmalig 299,00 € inkl. 19% MwSt.